Policy on Official Use Only Documents

1. Purpose

This policy establishes the requirements and standard practices for identifying, marking, and protecting certain documents containing a category of unclassified information known as Official Use Only (OUO) information.

2. Scope

This policy includes any document received from DOE marked as OUO, as well as any document produced by, for, or under the control of employees or users at Fermilab, which, by the nature of the document's content, potentially constitute OUO.

3. Applicability

This policy applies to Fermi Research Alliance, LLC and all its employees and Fermilab users.

4. Effective Date and Date Reviewed/Updated

This policy went into effect on September 11, 2020.

5. Policy

a. Identifying and categorizing OUO documents: For a document to be considered OUO it must present a risk of damage to government or private interest if improperly disclosed AND fall into a FOIA (Freedom of Information Act) exemption category, as fully described in the OUO Procedures Handbook. Employees or users who think a document requires OUO protection should consult with the OUO coordinator (listed in the Handbook) to determine proper categorization.

b. Marking of OUO documents: All documents containing OUO must be marked according to the rules in the OUO Procedures Handbook, except documents that are maintained in a restrictive access file. Such restricted access documents do not need marking as long as they are not copied, not shared, and returned to the restricted access file after each use. Any removable media containing OUO documents must also have some external marking identifying the media as containing OUO (and each document on the removable media must be appropriately marked).

c. Protection and storage of OUO documents, including control while in use:

- Protection in use: Reasonable precautions must be taken to prevent access to documents marked as OUO by persons who do not require the information to perform their jobs, as further explained in the OUO Procedures.
- Protection in storage: OUO documents must be stored either in offices where internal building security is maintained during off hours (for example by building access controls) or in receptacles that provide equivalent protection (for example in locked offices or locked file cabinets or desks).
- Protection on computing equipment: any stored copies of OUO material on IT equipment must provide methods (e.g., authentication, file access controls, passwords) to prevent access to OUO information by persons who do not require the information to perform their jobs.

d. Dissemination of OUO documents: OUO documents may only be shared with individuals who have a need to know the information to perform their job functions. This determination is made by each individual who has custody of an OUO document. That individual is responsible for ensuring that the recipient of the OUO document is aware of their responsibilities. Any copies of OUO documents must maintain the required markings.

e. Transmission of OUO documents: rules governing transmission of OUO by hand, physical mail, email, and fax are specified in the OUO Procedures Handbook. In general a sufficient level of encryption and obfuscation to ensure the document is not exposed to an unintended recipient is required.

f. Destruction of OUO documents: if an OUO document is to be shredded, or if it is determined to no longer contain OUO information, the procedures in the OUO Procedures Handbook must be followed.

g. Penalties for misuse of OUO material: misuse of OUO includes: release of any OUO information or document marked OUO to an individual who does not need to know that information to perform their job function; failure to mark as OUO a document knowingly containing OUO; and marking a document as OUO that is known to not contain any OUO. Employees found conducting any of these actions will be subject to administrative penalties, up to and including termination, determined by their supervisor and laboratory HR representatives.

6. Definitions

Official Use Only ("OUO") Document: A document containing information falling into certain specific categories that may have the potential to damage governmental, commercial, or private interests if it disseminated to persons who do not need the information to perform their job functions.

7. Responsibilities

The Fermilab OUO coordinators are responsible for managing the designation of documents within their area of expertise as OUO, and advising employees as to whether particular documents should be so characterized. These coordinators are identified in the OUO Procedures Handbook.

All employees are responsible for:

- Following rules governing protection, dissemination, and transmission of OUO documents of any come into their possession
- Consulting with lab OUO coordinators with questions about whether a particular document contains OUO

WDRS is responsible for determining the extent of administrative penalties imposed on an employee for misuse of OUO.

8. Authorities

DOE Order O471.3, dated 1-13-2011

DOE M 471.3-1, Manual for Identifying and Protecting Official Use Only Information, dated 1-13-2011

10 CFR Part 1004, Freedom of Information.

9. Owner

The Chief Information Officer is the owner of this policy.

10. Review Cycle

This policy shall be reviewed every three years or sooner if the DOE OUO Order is updated or superseded by an order about Controlled Unclassified information (CUI).

11. Communication Plan

The requirements of this policy shall be communicated to all employees, and periodic training shall be provided to Management System Owners, Chiefs/Division Heads/Section Heads/Project Directors, and employees who deal with categories of information that may be classified as OUO. This policy shall be available online in the Fermilab policy database. The Chief Information Officer is responsible for communicating this policy to all employees.